8

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/741,406	12/19/2000	James W. Edwards	10559/295001/P9306	6308

20985 7590 06/07/2005

FISH & RICHARDSON, PC
12390 EL CAMINO REAL
SAN DIEGO, CA 92130-2081

EXAMINER	
REVAK, CHRISTOPHER A	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 06/07/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

	Application No.	Applicant(s)	
Office Action Summary	09/741,406	EDWARDS ET AL.	
	Examiner	**Art Unit**	
	Christopher A. Revak	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 March 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5-12,14-26 and 28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5-12,14-26 and 28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

DETAILED ACTION

Response to Arguments

1. Applicant's arguments filed March 23, 2005 have been fully considered but they are not persuasive.

The applicant has argued that the examiner acknowledges that a "server" is not disclosed in the teachings of Gilbrech et al. This assertion is incorrect, the examiner is broadly interpreting the term "server" as being a computing device, such as a general purpose computer, such as a router in the teachings of Gilbrech et al wherein it "hosts" or "serves" as a connection point for all traffic to and from the LAN. The applicant has not claimed specific language to distinguish a server from this meaning. For arguments sake, the teachings of Gilbrech disclose of multiple local area networks, or LANs, as shown in Figure 2. Servers are notoriously well known to control access to the LANs and its resources and to govern communications from and to the LAN across a public network. The applicant's argument is moot.

The applicant has argued that the VPNUs disclosed in Gilbrech do not perform the same functions of a server component. The applicant has argued that Gilbrech et al will not work on "real private network environments such as a home private network." In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., home private network) are not recited in the rejected claims. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Gilbrech et al does disclose of multiple LANs, or private networks, please refer to Figure 2.

It is then stated by the applicant that Gilbrech et al discloses that the VPNU should be in the path of data traffic and resides between a site's router and the path to the Internet, or public network and the VPNUs should be bi-directional. It is argued that claim 1 does not require a VPN-type agent residing at the remote client side and the VPN-type agent cannot have the same functionality as claim 1. Applicant's arguments fail to comply with 37 CFR 1.111(b) because they amount to a general allegation that the claims define a patentable invention without specifically pointing out how the language of the claims patentably distinguishes them from the references. It is argued of "functionality" and the applicant has not expressively recited this functionality at question rendering the applicant's arguments moot.

It is additionally argued that Gilbrech et al can only secure communications between VPNUs and there exist nothing in the teachings of Gilbrech et al to secure communications between a server and a VPNU. The examiner disagrees, the teachings of Gilbrech et al show a dedicated connection between the router (server component) and a VPNU wherein the VPNU is responsible for enforcing authentication and encryption rules, please refer to column 8, lines 19-26 and as shown in Figure 2. It is interpreted that this connection is secure since it is monitored prior to being allowed to pass to the router (server component).

It is argued that Gilbrech et al uses fixed IP addresses in which the examiner agrees with the applicant's assertion. The argued new limitations recite of dynamically assigned addresses for agent component. The examiner notes that this limitation is admitted prior art based on the applicant's disclosure, please refer to the specification on page 2, lines 7-10.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-3,5-12,14-26, and 28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gilbrech et al in view of applicant's admitted prior art.

As per claim 1, it is disclosed by Gilbrech et al of a method comprising sending a packet originating from a source (device) across the Internet (public network) to a receiving VPN Unit (agent component) to establish a connection between the source (device) and a LAN (private network)(col. 6, lines 38-41; col. 8, lines 29-55; and as shown in Figures 2 & 5). A persistent connection is established between a router (server component) and a VPN Unit (agent component) since communications are necessary in order for the two to communicate (as shown in Figure 2) and this connection remains active as long as the devices maintain communications with one another unless if that connection is terminated by any or all of the devices. The router (server component) is configured to connect to the VPN Unit (agent component) prior to connecting to the enterprise (private) network (col. 2, lines 45-53, col. 6, lines 33-37, and as shown in Figure 2). It is determined if the communications from the device conform to authentication (authorization) rules to connect with the LAN (private network)(col. 2, lines 57-67). The request initiates from a router (first component) and is forwarded to a VPN Unit (agent component) to establish the connection with the destination (col. 2, lines 43-53,57-67 & col. 8, lines 17-26). The router (server component) creates and establishes the connection between the LAN (private network) and source (device) via the VPN Unit (agent component)(col. 9, line 55 through col. 10, line 10 & as shown in Figures 2 & 5) wherein the router (server component) receive transmitted messages and forward them to their correct destination, namely the LAN (private network) in light of the teachings of Gilbrech et al (as shown in Figures 2 & 5). The router (server component) is configured to connect to the VPN Unit (agent component) prior to connecting to the enterprise (private) network (col. 2, lines 45-53, col. 6, lines 33-37, and as shown in Figure 2). The router (server component) is configured with a persistent address (col. 8, lines 29-31). The teachings of Gilbrech et al are silent in disclosing that agent component is configured with a dynamically assigned IP address. The applicant's admitted prior art discloses that a contact point, such as a gateway device (agent component) is configured with a dynamically assigned IP address (page 2, lines 7-10). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply dynamic assigned IP addresses. The applicant's admitted prior art discloses motivation for use of dynamic

IP addresses by reciting it prevents or hinders devices on the Internet from establishing connections to a private network (page 2, lines 5-7). It would have been obvious to apply this feature to the teachings of Gilbrech et al as a means of further protecting the private network from unauthorized users establishing connections to the private network.

As per claims 2 and 11, Gilbrech et al discloses of forwarding a request initiated by a router (second/server component) and is forwarded to a VPN Unit (first/agent component) to establish the connection with the destination (col. 2, lines 43-53,57-67 & col. 8, lines 17-26). The examiner is interpreting the connection between the source (device), VPN Unit (first/agent component), router (second/server component), and device(s) on the LAN (private network) to remain active as long as the devices maintain communications with one another and that the connection is temporary until terminated.

As per claims 3 and 12, Gilbrech et al discloses of determining if the communications from the device conform with authentication rules to connect with the LAN and if so forwarding a request initiated by a router (second/server component) and is forwarded to a VPN Unit (first/agent component) to establish the connection with the destination (col. 2, lines 43-53,57-67 & col. 8, lines 17-26). If the request is not from a recognized member of the VPN group, the packets are discarded (denying the device access)(col. 2, lines 57-67 & col. 8, lines 12-27).

As per claims 5,6,14,15,25, and 26, it is disclosed by Gilbrech et al of a method comprising sending a packet originating from a source (device) across the Internet (public network) to a receiving VPN Unit (first/agent component) to establish a connection between the source (device) and a LAN (private network)(col. 6, lines 38-41; col. 8, lines 29-55; and as shown in Figures 2 & 5). The router (second/server component) is configured to connect to the VPN Unit (first/agent component) prior to connecting to the enterprise (private) network (col. 2, lines 45-53, col. 6, lines 33-37, and as shown in Figure 2). It is determined if the communications from the device conform to authentication (authorization) rules to connect with the LAN (private network)(col. 2, lines 57-67). The request initiates from a router (second/server component) and is forwarded to a VPN Unit (first/agent component) to establish the connection with the destination (col. 2, lines 43-53,57-67 & col. 8, lines 17-26). The router (second/server component) creates and establishes the connection between the LAN (private network) and source (device) via the VPN Unit (first/agent component)(col. 9, line 55 through col. 10, line 10 & as shown in Figures 2 & 5). The examiner is interpreting the connection between the source (device), VPN Unit (first/agent component), and router (second/server component) to remain active as long as the devices maintain communications with one another unless if that connection is terminated by any or all of the devices.

As per claims 7 and 16, Gilbrech et al discloses of determining if the communications from the device conform to authentication (authorization) rules to connect with the LAN (private network)(col. 2, lines 57-67). The request initiates from a router (second/server component) and is forwarded to a VPN Unit (first/agent component) to establish the connection with the destination (col. 2, lines 43-53,57-67 &

col. 8, lines 17-26). The examiner is interpreting the authentication rules to include a password since passwords are generally used for authentication.

As per claims 8, 17, and 23, it is recited by the teachings of Gilbrech et al that the public network includes the Internet (col. 2, lines 43-46).

As per claims 9 and 18, Gilbrech et al teaches of determining if the communications from the device conform to authentication (authorization) rules to connect with the LAN (private network)(col. 2, lines 57-67). The request initiates from a router (second/server component) and is forwarded to a VPN Unit (agent/first component) to establish the connection with the destination (col. 2, lines 43-53,57-67 & col. 8, lines 17-26). It is interpreted by the examiner that the VPN Unit (first/agent component) and router (second/server component) are proxy servers since it is disclosed in the applicant's specification "Proxy servers can monitor and intercept any and all requests being sent to and/or received from the private network and/or the Internet. The proxying components can also provide client-to-private-network encryption" as is recited on page 7, lines 13-17. Gilbrech discloses of performing encryption services on the packets and shows how both the VPN Unit (first/agent network component) and router (second/server component) intercept communications since that is the only path into the LAN (private network)(col. 8, lines 19-26 & as shown in Figure 2).

As per claim 10, it is disclosed by Gilbrech et al of a techniques (machine readable instructions stored on an article) for sending a packet originating from a source (device) across the Internet (public network) to a receiving VPN Unit (first component) to establish a connection between the source (device) and a LAN (private network)(col. 6, lines 38-41; col. 8, lines 29-55; and as shown in Figures 2 & 5). The router (second component) is configured to connect to the VPN Unit (first component) prior to connecting to the enterprise (private) network (col. 2, lines 45-53, col. 6, lines 33-37, and as shown in Figure 2). It is determined if the communications from the device conform to authentication (authorization) rules to connect with the LAN (private network)(col. 2, lines 57-67). The request initiates from a router (second component) and is forwarded to a VPN Unit (first component) to establish the connection with the destination (col. 2, lines 43-53,57-67 & col. 8, lines 17-26). The router (second component) creates and establishes the connection between the LAN (private network) and source (device) via the VPN Unit (first component)(col. 9, line 55 through col. 10, line 10 & as shown in Figures 2 & 5) and the router (second component) receives transmitted messages and forward them to their correct destination, namely the LAN (private network) in light of the teachings of Gilbrech et al (as shown in Figures 2 & 5). The router (second component) is configured to connect to the VPN Unit (first component) prior to connecting to the enterprise (private) network (col. 2, lines 45-53, col. 6, lines 33-37, and as shown in Figure 2). The teachings of Gilbrech et al are silent in disclosing that the first component is configured with a dynamically assigned IP address. The applicant's admitted prior art discloses that a contact point, such as a gateway device (first component) is configured with a dynamically assigned IP address (page 2, lines 7-10). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply dynamic assigned IP addresses. The applicant's admitted prior art discloses motivation for use of dynamic IP addresses by reciting it prevents or hinders devices on the Internet from establishing connections to a private network (page 2, lines 5-7). It would have been obvious to apply this feature to the teachings of Gilbrech et al as a means of further protecting the private network from unauthorized users establishing connections to the private network.

As per claim 19, it is disclosed by Gilbrech et al of a system for sending a packet originating from a source (device) across the Internet (public network) to a receiving VPN Unit (agent component) to establish a connection between the source (device) and a LAN (private network)(col. 6, lines 38-41; col. 8, lines 29-55; and as shown in Figures 2 & 5). The VPN Unit (server component) establishes the connection with the destination (col. 2, lines 57-67 & col. 8, lines 17-26). The request is then forwarded from the VPN Unit (agent component) to the router (server component)(col. 8, lines 52-55 & as shown in Figures 2 & 5). The router (server component) creates and establishes the connection between the LAN (private network) and source (device) via the VPN Unit (agent component)(col. 9, line 55 through col. 10, line 10 & as shown in Figures 2 & 5) and router (server component) receive transmitted messages and forward them to their correct destination, namely the LAN (private network) in light of the teachings of Gilbrech et al (as shown in Figures 2 & 5). The router (server component) is configured to connect to the VPN Unit (server component) prior to connecting to the enterprise (private) network (col. 2, lines 45-53, col. 6, lines 33-37, and as shown in Figure 2). The teachings of Gilbrech et al are silent in disclosing that agent component is configured with a dynamically assigned IP address. The applicant's admitted prior art discloses that a contact point, such as a gateway device (agent component) is configured with a dynamically assigned IP address (page 2, lines 7-10). It would have been obvious to a person of ordinary skill in the art at the time of the invention to have been motivated to apply dynamic assigned IP addresses. The applicant's admitted prior art discloses motivation for use of dynamic IP addresses by reciting it prevents or hinders devices on the Internet from establishing connections to a private network (page 2, lines 5-7). It would have been obvious to apply this feature to the teachings of Gilbrech et al as a means of further protecting the private network from unauthorized users establishing connections to the private network.

As per claim 20, Gilbrech et al discloses of a router (server component) that creates and establishes the connection between the LAN (private network) and source (device) via the VPN Unit (agent component)(col. 9, line 55 through col. 10, line 10 & as shown in Figures 2 & 5) and router (server component) receives transmitted messages and forward them to their correct destination, namely the any devices within the LAN (private network) as is taught by Gilbrech et al (as shown in Figures 2 & 5).

As per claims 20 and 21, Gilbrech et al teaches of forwarding a request from the VPN Unit (agent component) to the router (server component)(col. 8, lines 52-55 & as shown in Figures 2 & 5). The router (server component) creates and establishes the connection (by providing access) between the LAN (private network) and source (device) via the VPN Unit (agent component)(col. 9, line 55 through col. 10, line 10 & as shown in Figures 2 & 5). Figure 2 shows multiple devices connected to the LAN (private network).

As per claim 22, it is disclosed by Gilbrech et al that communications are extensible to support any protocol used by the Internet (public network) and the LAN (private network)(col. 5, lines 57-61 & col. 6, lines 5-22). It is interpreted by the examiner that the VPN Unit (agent component) and router (server component) handle the different protocols since they are connected across the Internet (public network) and LAN (private network)(as shown in Figures 2 & 5).

As per claim 24, Gilbrech et al teaches of determining if the communications from the device conform to authentication rules to connect with the LAN and if so, the VPN Unit (agent component) establishes the connection with the destination (col. 2, lines 57-67 & col. 8, lines 17-26).

As per claim 28, it is shown in Figure 2 of Gilbrech et al the routers (server components) are implemented inside the LANs (private networks).

Conclusion

4. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher A. Revak whose telephone number is 571-272-3794. The examiner can normally be reached on Monday-Friday, 6:30am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher Revak
AU 2131

6/5/05

CR
June 5, 2005